#5

Docket No.826.1670 (JDH)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:)
)
Nobuyuki MORI, et al.)
) Group Art Unit: Unassigned
Serial No.: To be assigned)
) Examiner: Unassigned
Filed: January 30, 2001)

For: **SIGNATURE SYSTEM PRESENTING USER SIGNATURE INFORMATION**

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. §1.55

Assistant Commissioner for Patents
Washington, D.C. 2023l

Sir:

In accordance with the provisions of 37 C.F.R. §1.55, the applicants submit herewith a certified copy of the following foreign application:

Japanese Patent Application No. 10-220658
Filed: August 4, 1998.

It is respectfully requested that the applicant s be given the benefit of the foreign filing date as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. §119.

Respectfully submitted,

STAAS & HALSEY LLP

By:_____
James D. Halsey, Jr.
Registration No. 22,729

700 11th Street, N.W., Ste. 500
Washington, D.C. 20001
(202) 434-1500
Date: January 30, 2001

W:\826\1670\priority.wpd

PATENT OFFICE

JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this office.

Date of Application: August 4, 1998

Application Number: Patent Application No. 10-220658

Applicant(s): FUJITSU LIMITED,
The Sakura Bank, Limited

December 22, 2000

Commissioner,
Patent Office Kozo Oikawa

Certificate No. 2000-3105861

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９８年 ８月 ４日

出 願 番 号
Application Number: 平成１０年特許願第２２０６５８号

出 願 人
Applicant (s): 富士通株式会社
株式会社さくら銀行

２０００年１２月２２日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号 出証特２０００－３１０５８６１

【書類名】　特許願

【整理番号】　9804118

【提出日】　平成10年 8月 4日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 17/60

【発明の名称】　署名システム

【請求項の数】　21

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　森　信行

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　宮坂　道弘

【発明者】

【住所又は居所】　東京都千代田区九段南１丁目３番１号　株式会社さくら銀行内

【氏名】　山口　隆之

【特許出願人】

【識別番号】　000005223

【氏名又は名称】　富士通株式会社

【特許出願人】

【識別番号】　596089344

【氏名又は名称】　株式会社さくら銀行

【代理人】

【識別番号】　100074099

【郵便番号】　102

【住所又は居所】　東京都千代田区二番町８番地２０　二番町ビル３Ｆ

【弁理士】

【氏名又は名称】　大菅　義之

【電話番号】　03-3238-0031

【選任した代理人】

【識別番号】　100067987

【郵便番号】　222

【住所又は居所】　神奈川県横浜市港北区太尾町１４１８－３０５（大倉山二番館）

【弁理士】

【氏名又は名称】　久木元　彰

【電話番号】　045-545-9280

【手数料の表示】

【予納台帳番号】　012542

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【物件名】　委任状　1

【包括委任状番号】　9705047

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　署名システム

【特許請求の範囲】

【請求項１】　利用者の署名情報を受領者に提示する署名システムであって、

前記利用者の識別情報を入力する入力手段と、

入力された識別情報に基づいて、前記署名情報を生成するための情報を、バーコードリーダに読み取られる形式で出力する出力手段と

を備えることを特徴とする署名システム。

【請求項２】　前記出力手段は、前記識別情報を暗号化して出力することを特徴とする請求項１記載の署名システム。

【請求項３】　前記入力手段は、前記利用者が繰り返し再現することのできる意味のある本人情報を、前記識別情報として入力することを特徴とする請求項１記載の署名システム。

【請求項４】　前記入力手段は、印影の画像データを前記識別情報として入力することを特徴とする請求項１記載の署名システム。

【請求項５】　前記出力手段は、不正使用を防止するための不正使用防止情報を生成するためのプログラム情報を出力することを特徴とする請求項１記載の署名システム。

【請求項６】　前記プログラム情報は、一方向性関数を含み、該一方向性関数を用いて使用情報のブラインド情報を生成し、該ブラインド情報を含む前記不正使用防止情報を生成するために用いられることを特徴とする請求項５記載の署名システム。

【請求項７】　前記プログラム情報は、暗号キーを含み、該暗号キーを用いて使用情報のブラインド情報を生成し、該ブラインド情報を含む前記不正使用防止情報を生成するために用いられることを特徴とする請求項５記載の署名システム。

【請求項８】　利用者の署名情報を受領者に提示する署名システムであって、

バーコード形式の情報を読み取る読取手段と、

読み取られた情報に基づいて、前記署名情報を生成する生成手段と

を備えることを特徴とする署名システム。

【請求項９】　前記生成手段は、前記読み取られた情報に、不正使用を防止するための不正使用防止情報を付加して、前記署名情報を生成することを特徴とする請求項８記載の署名システム。

【請求項１０】　前記読み取り手段は、前記署名情報を生成するためのプログラム情報を読み取り、前記生成手段は、該プログラム情報を用いて前記不正使用防止情報を生成することを特徴とする請求項９記載の署名システム。

【請求項１１】　前記不正使用防止情報として用いるための日時情報を生成するタイマ手段をさらに備えることを特徴とする請求項９記載の署名システム。

【請求項１２】　前記バーコード形式の情報に含まれる識別情報のブラインド情報を管理する管理手段と、前記署名情報から該識別情報のブラインド情報を生成し、得られたブラインド情報を該管理手段が管理するブラインド情報と比較する比較手段とをさらに備えることを特徴とする請求項８記載の署名システム。

【請求項１３】　前記識別情報のブラインド情報を含む証明情報を発行する発行手段をさらに備えることを特徴とする請求項１２記載の署名システム。

【請求項１４】　利用者が繰り返し再現できる意味のある本人情報を入力する入力手段と、

前記本人情報のブラインド情報を生成する生成手段と、

前記本人情報に基づく署名情報を検証する装置に、前記ブラインド情報を登録する登録手段と

を備えることを特徴とする署名システム。

【請求項１５】　前記入力手段および生成手段は、前記利用者の端末上に設けられることを特徴とする請求項１４記載の署名システム。

【請求項１６】　前記利用者が前記署名情報を受領者に提示する際、該利用者は、前記入力手段を用いて前記本人情報を再入力し、前記生成手段は、再入力された本人情報から該署名情報を生成することを特徴とする請求項１４記載の署名システム。

【請求項１７】　前記入力手段は、前記利用者との対話形式により、複数の項目の中から前記本人情報を選択的に入力することを特徴とする請求項１４記載の署名システム。

【請求項１８】　前記入力手段は、前記署名情報の用途に応じて、前記本人情報の入力項目数を変更することを特徴とする請求項１７記載の署名システム。

【請求項１９】　コンピュータのためのプログラムを記録した記録媒体であって、

利用者の識別情報を入力するステップと、

入力された識別情報に基づいて、前記利用者の署名情報を生成するための情報を生成するステップと、

生成された情報を、バーコードリーダに読み取られる形式で出力するステップと

を含む処理を前記コンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項２０】　コンピュータのためのプログラムを記録した記録媒体であって、

バーコード形式の情報を読み取るステップと、

読み取られた情報に基づいて、利用者の署名情報を生成するステップと

を含む処理を前記コンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項２１】　コンピュータのためのプログラムを記録した記録媒体であって、

利用者が繰り返し再現できる意味のある本人情報を入力するステップと、

前記本人情報のブラインド情報を生成するステップと、

前記本人情報に基づく署名情報を検証する装置に、前記ブラインド情報を登録するステップと

を含む処理を前記コンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、配送された品物の受け取り、金融機関との取引、他人との取引等において、利用者が本人であることを示す情報を相手に提示する署名システムに関する。

【０００２】

【従来の技術とその問題点】

我が国を含むアジア諸国では、伝統的に、書類に署名・押印することにより、署名者が本人であることを相手に示す習慣がある。例えば、我が国では、不動産取引等の重要な取引には実印が用いられ、銀行との取引には銀行印が用いられ、宅配された品物の受け取りには認印が用いられる。取引に印鑑を用いることのない国々では、自筆署名が用いられるのが一般的である。

【０００３】

しかしながら、署名は他人が模倣することも可能であり、その筆跡を正確に識別するためには、専門家の鑑定を要する。また、印鑑は偽造することができ、印影を正確に識別するには、署名の筆跡と同様に、専門家の鑑定を要することが多い。したがって、署名や押印が不正に行われた場合、書類の受領者は本人確認を行うことが困難である。

【０００４】

また、近年盛んに研究されているコンピュータネットワークを利用した電子商取引においては、自筆署名や印鑑を直接用いることができない。なぜならば、書類の受領者にとって、相手がその書類に記載された人物自身であるかどうか、即ちコピーによる不正使用か否かを確認することが一層困難となるからである。

【０００５】

従来の金融機関（銀行等）のＡＴＭ（Automatic Teller Machine）では、取引相手の利用者を識別するために暗証番号を用いている。しかし、暗証番号として、利用者の電話番号や生年月日等の意味のある情報を用いた場合、それが他の紙媒体等に記載されていることが多く、簡単に推定され、不正使用されやすい。また、ランダムな数字列等の意味のない情報を暗証番号として用いた場合、本人が

いつまでも正確に記憶していることは困難である。このため、本人が紙媒体等に記録しておくことが多く、盗用される可能性がある。

【０００６】

さらに、金融機関では、入力された暗証番号を照合するため、マスターデータベース等の媒体に暗証番号を保存して管理しており、その媒体が不正にアクセスされて、暗証番号が盗用される危険性もある。

【０００７】

本発明の課題は、情報処理装置を用いて利用者の識別情報を相手に提示し、それを安全に管理する署名システムを提供することである。

【０００８】

【課題を解決するための手段】

図１は、本発明の署名システムの原理図である。図１の署名システムは、入力手段１、出力手段２、読取手段３、および生成手段４を備え、利用者の署名情報を受領者に提示する。

【０００９】

本発明の第１の原理によれば、入力手段１は、利用者の識別情報を入力する。そして、出力手段２は、入力された識別情報に基づいて、署名情報を生成するための情報を、バーコードリーダに読み取られる形式で出力する。

【００１０】

利用者の識別情報は、例えば、利用者が繰り返し再現することのできる意味のある情報や、利用者の印鑑の印影等であり、デジタルデータとして入力されて管理される。そして、この識別情報に基づいて、署名情報を生成するために必要な情報が生成され、生成された情報はバーコード形式で出力される。例えば、出力情報には、利用者の識別情報と、識別情報を用いて署名情報を生成するプログラムの情報が含まれる。

【００１１】

本発明の第２の原理によれば、読取手段３は、バーコード形式の情報を読み取る。そして、生成手段４は、読み取られた情報に基づいて、署名情報を生成する。

【００１２】

読取手段３は、出力手段２により出力された情報を読み取る。また、生成手段４は、例えば、読み取られた情報に含まれるプログラムを実行して、利用者の識別情報を含む署名情報を生成し、それを受領者に提示する。

【００１３】

このような署名システムによれば、署名情報を生成するための情報は、バーコード形式で出力されて受領者に渡されるため、人間がその内容を理解することは極めて困難である。したがって、自筆署名や印鑑を用いる場合に比べて、他人が不正に使用することが難しく、より高い安全性が得られる。また、利用者が入力した識別情報をそのまま署名情報として用いるのではなく、それに情報を付加して署名情報を生成すれば、安全性はさらに向上する。

【００１４】

さらに、利用者の識別情報としては、バーコードの容量の範囲で可能な複雑な情報を用いることができ、従来の暗証番号と比べて、他人が推定することが難しくなる。したがって、利用者以外の人間が正しい識別情報を入力して、署名情報を生成するための情報を生成することは不可能に近い。

【００１５】

例えば、図１の入力手段１と出力手段２は、図２の端末１１に対応し、図１の読取手段３と生成手段４は、図２のバーコードリーダ１２および図１１のバーコードリーダ８２に対応する。また、例えば、署名情報を生成するための情報は、図２の２次元バーコード１４、１５に対応する。

【００１６】

【発明の実施の形態】

以下、図面を参照しながら、本発明の実施の形態を詳細に説明する。

本発明の署名システムでは、宅配等の品物を受領したり、取引書類等を提出したりするために、本人であることを示す署名情報を受領者の処理装置に提示する際、自筆署名や押印を行う代わりに、２次元バーコード等の上書き不可能な媒体に本人情報を記録して、処理装置に読み取らせる。

【００１７】

この本人情報は、利用者の頭の中に存在する意味のある情報であって、利用者がいつまでも正確に記憶していることができ、必要なときに繰り返し再現することができる。このため、利用者は本人情報を紙媒体等に記録しておく必要がなく、他人がそれを知ることは極めて困難である。

【００１８】

本人情報としては、例えば、利用者の個人情報（氏名、住所、電話番号、生年月日、趣味、特技、旧姓等）、利用者の家族構成、利用者の家系情報（祖先の個人情報等）、利用者が好きな言葉（熟語、格言、詩の一節、家訓等）、利用者が尊敬する人物名等の項目が考えられる。

【００１９】

安全性を高めるには、これらの項目のうち２種類以上を組み合わせて用いるのが望ましく、利用者は、使用する項目を取引の種類に応じて選択することができる。これらの項目の組み合わせ方により、本人情報の複雑さが変化し、デジタル署名（デジタル印鑑）としての用途を変更することが可能になる。利用者は、パーソナルコンピュータ等の端末を用いて、対話形式により、多数の項目の中から本人情報を選択的に入力し、用途に応じて入力項目数を変更する。

【００２０】

例えば、本人情報を実印の代わりに用いる場合は、３種類以上の項目を組み合わせてレベル１のデジタル署名を生成し、銀行印の代わりに用いる場合は、２種類の項目を組み合わせてレベル２のデジタル署名を生成し、認印の代わりに用いる場合は、１種類のみの項目を用いてレベル３のデジタル署名を生成することが可能である。また、３種類の４文字熟語のように、同じ項目に属する複数の情報を組み合わせることもできる。

【００２１】

２次元バーコードは、例えば、英数字の場合は２０００～３０００文字程度の情報を出力することができ、日本語の場合は６００～７００文字程度の情報を出力することができる。

【００２２】

さらに、本人情報を読み取った処理装置は、本人情報から署名情報を生成する

際に、他人による不正使用を防止するためのブラインド情報を動的に生成して、それを署名情報に埋め込む。ブラインド情報とは、与えられた情報をハッシュ関数等の一方向性関数により変換した結果、またはその結果を用いて生成される情報であり、ブラインド情報から元の情報を再生することはできない。

【００２３】

このブラインド情報を生成するためのプログラムは、利用者専用の一方向性関数と暗号キーを含み、２次元バーコードに記録されて、本人情報とともに処理装置に読み取られる。

【００２４】

処理装置は、２次元バーコードの情報を読み取る際、本人情報に対応するデジタルデータの動的書き込み領域と、ブラインド情報に対応するデジタルデータの記憶領域と、プログラムの記憶領域とを確保する。そして、２次元バーコードを読み取ると、本人情報を動的書き込み領域に書き込み、プログラムを記憶領域にロードする。

【００２５】

このプログラムは、読み込まれて実行されると、本人情報の動的書き込み領域内に、署名した年月日および時刻、または動的に求めた乱数のような再現性のないデータを、使用情報として書き込む。この使用情報は、本人情報が使用済みであることを表している。次に、使用情報に対して一方向性関数を適用し、適用結果を暗号キーを用いて暗号化してブラインド情報を生成し、それをブラインド情報の記憶領域に書き込む。

【００２６】

次に、プログラムは、これらの本人情報、使用情報、および使用情報のブラインド情報から署名情報を生成し、それを処理装置に保存した後、自らを記憶領域から削除する。さらに、受領者の名前等を使用情報に追加しておくと、署名情報の安全性がより高められる。

【００２７】

このような署名システムによれば、本人情報は署名情報に変換されて処理装置に保存され、平文の本人情報はどこにも保存されないので、他人がそれを不正に

使用することは極めて困難である。

【００２８】

また、受領者または第３者が、保存された署名情報をコピーしてそのまま他の目的に使用しても、既に使用済みであることを表す使用情報が付加されているため、不正使用であることが分かってしまう。さらに、受領者または第３者が署名情報をコピーして、使用情報を尤もらしい内容に書き換えても、それに対応するブラインド情報を生成することはできない。したがって、書き換えられた使用情報とブラインド情報を比較することで、不正使用であることが客観的に立証される。

【００２９】

このように、本発明では、利用者のみが繰り返し再現できる本人情報と、本人情報の不正使用を防止するための使用情報とを用いて署名情報を生成することで、自筆署名や印鑑を用いる場合よりも、各段に高い安全性が得られる。

【００３０】

図２は、２次元バーコードを用いた署名システムの構成図である。図２の署名システムは、利用者の端末１１（パーソナルコンピュータ等）、受領者のバーコードリーダ１２、および第３者の証明装置１３（サーバ等）を含む。

【００３１】

利用者は、受領者に対して本人であることを示す識別情報を提示する際、デジタルデータの署名情報を印鑑の代わりに使用できるように、必要な情報を端末１１上で２次元バーコード１４、１５に変換して管理する。また、署名情報を検証するために必要な情報を、ネットワークを介して証明装置１３のデータベース１６に登録しておく。２次元バーコード１４は上述の本人情報に対応し、２次元バーコード１５は上述のプログラムに対応する。

【００３２】

利用者から２次元バーコード１４、１５を提示されると、受領者は、バーコードリーダ１２を用いてそれらを読み取り、バーコードリーダ１２は、署名情報を生成して、利用者の本人確認を行う。このとき、バーコードリーダ１２は、ネットワークを介して証明装置１３に署名情報の検証を依頼し、検証結果を受け取っ

て受領者に提示する。

【００３３】

証明装置１３は、例えば、実印の印鑑登録証を発行する公的機関に対応し、データベース１６に登録された情報を用いて、第３者の立場で署名情報の正当性を立証する。したがって、証明装置１３を含む署名システムでは、本人情報が実印の代わりに用いられると考えられ、このシステムは、利用者と受領者が重要性の高い取引を行う場合に適している。

【００３４】

図３は、バーコードリーダ１２の構成図である。図３のバーコードリーダは、読取装置２１、通信装置２２、制御装置２３、記憶装置２４、表示装置２５、タイマ２６、および乱数発生器２７を備える。

【００３５】

読取装置２１は、２次元バーコード１４、１５の情報を読み取り、制御装置２３を介して記憶装置２４に入力する。通信装置２２は、ネットワークを介して証明装置１３等と通信し、表示装置２５は、必要な情報を受領者に提示する。タイマ２６は現在の日時情報を生成し、乱数発生器２７は乱数を発生する。日時情報および乱数は、上述の使用情報として用いられる。また、制御装置２３は、他の装置の動作を制御する。

【００３６】

図４および図５は、利用者が検証用の情報を証明装置１３に登録する処理を示している。まず、端末１１は、登録者である利用者が入力した本人情報３１にメッセージダイジェスト関数（ＭＤ関数）３２を適用して、メッセージダイジェスト（ＭＤ）３３を生成する。ＭＤ関数３２は、ハッシュ関数等の一方向性関数であって、ＭＤ３３から本人情報３１を再生することはできない。

【００３７】

次に、端末１１は、暗号キー３４を用いてＭＤ３３を暗号化し、ブラインド情報３５を生成する。暗号化アルゴリズムとしては、例えば、暗号化と復号化に同一の暗号キーを用いるＤＥＳ（Data Encryption Standard）が用いられる。端末１１は、ブラインド情報３５、ＭＤ関数３２、および暗号キー３４を証明装置１

３に送信し、証明装置１３は、それらの情報をデータベース１６に登録する。

【００３８】

また、登録者は、パスポートや運転免許証等の本人証明書３６の画像を端末１１に入力し、それを本人確認のために証明装置１３に送信する。本人確認が行われると、本人証明書３６は直ちに消去される。

【００３９】

次に、証明装置１３は、ブラインド情報３５が登録者のものかどうかを判定するために、本人情報３１を端末１１に要求する。これを受けて、登録者が本人情報３１を再入力すると、端末１１は、暗号キー３４を用いて本人情報３１を暗号化し、暗号化本人情報３７を生成して、証明装置１３に送信する。

【００４０】

証明装置１３は、データベース１６に保存された暗号キー３４を用いて暗号化本人情報３７を復号化し、平文の本人情報３８を得る。さらに、データベース１６に保存されたＭＤ関数３２を本人情報３８に適用してＭＤ３９を生成し、それを暗号キー３４で暗号化してブラインド情報４０を生成する。そして、得られたブラインド情報４０をデータベース１６に保存されたブラインド情報３５と比較する。

【００４１】

このとき、ブラインド情報４０とブラインド情報３５が一致すれば、登録処理が正常に終了したことを端末１１に通知する。また、両者が一致しなければ、データベース１６に登録された情報を無効にして、登録処理が中止されたことを端末１１に通知する。したがって、登録者が正しい本人情報３１を再入力した場合のみ、ブラインド情報３５、ＭＤ関数３２、および暗号キー３４がデータベース１６に登録される。また、本人情報３８、ＭＤ３９、およびブラインド情報４０は、使用後直ちに消去される。

【００４２】

次に、登録者が、本人であることを証明する証明書の発行を依頼すると、図６のような処理が行われる。まず、端末１１が証明書の発行依頼を証明装置１３に送信すると、証明装置１３は本人情報３１を端末１１に要求する。これを受けて

、端末１１は、暗号キー３４を用いて本人情報３１を暗号化し、暗号化本人情報４１を生成して、証明装置１３に送信する。

【００４３】

証明装置１３は、図５と同様の処理を行って、暗号化本人情報４１を検証する。まず、データベース１６に保存された暗号キー３４を用いて暗号化本人情報４１を復号化し、平文の本人情報４２を得る。さらに、データベース１６に保存されたＭＤ関数３２を本人情報４２に適用してＭＤ４３を生成し、それを暗号キー３４で暗号化してブラインド情報４４を生成する。そして、得られたブラインド情報４４をデータベース１６に保存されたブラインド情報３５と比較する。

【００４４】

このとき、ブラインド情報４４とブラインド情報３５が一致すれば、証明書の発行日時、発行機関名、有効期間等を付加情報４５としてブラインド情報４４に付加し、証明情報４６を生成する。そして、証明情報４６を端末１１に送信し、付加情報４５をデータベース１６に登録して、処理を終了する。本人情報４２、ＭＤ４３、およびブラインド情報４４は、使用後直ちに消去される。ブラインド情報４４とブラインド情報３５が一致しなければ、依頼者が登録者とは異なるものとみなし、証明情報４６は発行しない。

【００４５】

このように、証明装置１３は、利用者のＭＤ関数３２と暗号キー３４を保存することで、いつでも与えられた本人情報からブラインド情報を生成することができ、それをブラインド情報３５と比較して本人情報が正しいかどうかを判定することができる。

【００４６】

次に、利用者が２次元バーコードを受領者に提示する場合の処理について説明する。図７は、証明情報４６を含む２次元バーコードの読取処理を示している。利用者が本人情報３１を入力すると、端末１１は、図６の暗号化本人情報４１と同様にして暗号化本人情報５１を生成し、それを証明情報４６とともに２次元バーコード１４に出力する。また、ＭＤ関数３２と暗号キー３４を含む署名プログラム５２を２次元バーコード１５に出力する。

【００４７】

バーコードリーダ１２は、２次元バーコード１４、１５の情報を読み取って記憶装置２４の記憶領域に格納した後、署名プログラム５２を実行する。署名プログラム５２は、まず、タイマ２６または乱数発生器２７から日時データまたは乱数データを取得し、それを使用情報５３とする。次に、使用情報５３にＭＤ関数３２を適用してＭＤ５４を生成し、それを暗号キー３４で暗号化してブラインド情報５５を生成する。

【００４８】

そして、暗号化本人情報５１、証明情報４６、使用情報５３、およびブラインド情報５５をまとめて署名情報５６を生成し、それを記憶装置２４に格納する。その後、記憶装置２４内の署名プログラム５２を自ら消去して、処理を終了する。

【００４９】

バーコードリーダ１２は、署名情報５６に含まれる暗号化本人情報５１および証明情報４６から平文の本人情報３１を再生することができないため、署名情報５６の正当性を検証することはできない。そこで、受領者の希望に応じて、署名情報５６の検証を証明装置１３に依頼する。

【００５０】

図８は、このような検証処理を示している。バーコードリーダ１２が署名情報５６とともに検証依頼を証明装置１３に送信すると、証明装置１３は、署名情報５６から暗号化本人情報５１、証明情報４６、使用情報５３、およびブラインド情報５５を取り出す。

【００５１】

証明装置１３は、まず、暗号キー３４で暗号化本人情報５１を復号化して平文の本人情報５７を生成し、本人情報５７にＭＤ関数３２を適用してＭＤ５８を生成し、それを暗号キー３４で暗号化してブラインド情報５９を生成する。そして、得られたブラインド情報５９をデータベース１６に保存されたブラインド情報３５と比較する。

【００５２】

ブラインド情報５９とブラインド情報３５が一致すれば、次に、証明情報４６をブラインド情報６０と付加情報６１に分解し、ブラインド情報６０をブラインド情報３５と比較し、付加情報６１をデータベース１６に保存された付加情報４５と比較する。

【００５３】

ブラインド情報６０とブラインド情報３５が一致し、付加情報６１と付加情報４５が一致すれば、次に、使用情報５３にＭＤ関数３２を適用してＭＤ６２を生成し、それを暗号キー３４で暗号化してブラインド情報６３を生成する。そして、得られたブラインド情報６３をブラインド情報５５と比較する。

【００５４】

ブラインド情報６３とブラインド情報５５が一致すれば、署名情報５６は利用者の正しい識別情報を表しているものとみなし、その旨をバーコードリーダ１２に通知する。

【００５５】

また、ブラインド情報５９とブラインド情報３５が一致しない場合、ブラインド情報６０とブラインド情報３５が一致しない場合、付加情報６１と付加情報４５が一致しない場合、またはブラインド情報６３とブラインド情報５５が一致しない場合は、署名情報５６が正しくないものとみなし、その旨をバーコードリーダ１２に通知する。本人情報５７、ＭＤ５８、およびブラインド情報５９は、使用後直ちに消去される。

【００５６】

秘密キー／公開キーアルゴリズムを利用した従来の認証局による本人証明方法では、利用者のＭＤ関数、公開キー、個人情報等が公開され、プライバシーが保護されないことが多い。また、利用者は、秘密キーを個人責任で管理しなければならず、常に、デジタル署名を確認しながら相手と通信する必要がある。

【００５７】

これに対して、図２の署名システムでは、必要最小限の情報が平文として登録され、元の本人情報３１はそのままでは登録されずに、他人が認識できないブラインド情報３５の形で登録される。したがって、利用者のプライバシーが保護さ

れ、他人による本人情報３１の盗用が防止される。

【００５８】

また、図７の２次元バーコード１４に、利用者と受領者の間の取引に関する情報を記述しておき、証明装置１３が両者に代わって取引の決済を行うこともできる。この場合、受領者は、バーコードリーダ１２の表示装置２５を利用して、２次元バーコード１４から読み込まれた取引情報を確認し、内容が正しければ、署名情報５６の検証を証明装置１３に依頼する。

【００５９】

そして、証明装置１３は、署名情報５６が正しいと判定すると、その取引に関する決済を行う。これにより、例えば、金融機関に設けられた利用者と受領者の口座間で金銭情報が移転される。

【００６０】

ところで、図２の署名システムでは、利用者は第３者が発行する証明情報４６を２次元バーコード１４に出力しているが、宅配業者からの品物の受け取り等のより重要性の低い取引の場合は、必ずしも証明情報４６や証明装置１３は必要ではない。また、本人情報３１としてより簡単な情報を用いることができ、必ずしもそれを暗号化して２次元バーコード１４に出力する必要はない。

【００６１】

図９は、証明情報４６を含まない２次元バーコードの読取処理を示している。利用者が本人情報３１を入力すると、端末１１は、それを２次元バーコード１４に出力し、ＭＤ関数３２と暗号キー３４を含む署名プログラム７１を２次元バーコード１５に出力する。

【００６２】

ここでは、利用者およびその家族が２次元バーコードを認印の代わりに使用する場合を想定し、利用者自身が使用する場合は、氏名、住所、電話番号等の個人情報を本人情報３１として用い、家族が使用する場合は、名字のみを本人情報３１として用いることにする。

【００６３】

バーコードリーダ１２は、２次元バーコード１４、１５の情報を読み取って記

憶装置２４の記憶領域に格納した後、署名プログラム７１を実行する。署名プログラム７１は、テスト情報７２、本人情報３１、および使用情報７３のブラインド情報を生成する。テスト情報７２は、ＭＤ関数３２と暗号キー３４をテストするための適当な情報であり、使用情報７３は、例えば、タイマ２６から取得した日時データである。

【００６４】

まず、テスト情報７２、本人情報３１、および使用情報７３のそれぞれにＭＤ関数３２を適用し、ＭＤ７４、７５、７６を生成し、次に、暗号キー３４でそれらを暗号化してブラインド情報７７、７８、７９を生成する。ここで、ブラインド情報７７、７８、７９は、それぞれ、平文のテスト情報７２、本人情報３１、使用情報７３に対応するブラインド情報である。

【００６５】

そして、テスト情報７２、本人情報３１、使用情報７３、およびブラインド情報７７、７８、７９をまとめて署名情報８０を生成し、それを記憶装置２４に格納した後、記憶装置２４内の署名プログラム７１を自ら消去して、処理を終了する。

【００６６】

図１０は、記憶装置２４の記憶領域に格納された署名情報８０を示している。図１０において、アドレスａ１、ａ２、ａ３、ａ４、ａ５、ａ６に、それぞれ、テスト情報７２、本人情報３１、使用情報７３、ブラインド情報７８、７９、７７が格納されている。２次元バーコード１４、１５の読み取り前には、アドレスａ３に、未使用であることを示す情報が書き込まれており、それが読み取り時の日時データに書き換えられる。

【００６７】

この署名システムにおいては、受領者または第３者が、保存された署名情報をコピーして他の目的に使用しても、現在の日時と使用情報の日時が異なるため、不正使用であることが分かってしまう。さらに、受領者または第３者が使用情報の日時を現在の日時に変更して使用しても、それに対応するブラインド情報を生成することはできない。したがって、書き換えられた使用情報とブラインド情報

を比較することで、不正使用であることが立証される。

【００６８】

次に、利用者が２次元バーコードを用いて、銀行等の金融機関と取引を行うための署名システムについて説明する。図１１は、このような署名システムの構成図である。図１１の署名システムは、利用者の端末１１、金融機関の金融処理装置８１（サーバ等）、および金融機関のバーコードリーダ８２を含む。バーコードリーダ８２は、図３と同様の構成を有する。

【００６９】

利用者は、金融機関に取引書類を提出する際、デジタルデータの署名情報を印鑑の代わりに使用できるように、必要な情報を端末１１上で２次元バーコード１４、１５に変換して管理する。また、署名情報を検証するために必要な情報を、ネットワークを介して金融処理装置８１のデータベース８３に登録しておく。

【００７０】

金融処理装置８１へ情報を登録する処理は、図４および図５に示した処理と同様である。あらかじめ証明装置１３から図６の証明情報４６が発行されている場合は、図４において、本人確認のために本人証明書３６を送信する代わりに、証明情報４６を送信してもよい。

【００７１】

利用者から２次元バーコード１４、１５を提示されると、バーコードリーダ８２は、それらを読み取り、署名情報を生成して、利用者の本人確認を行う。２次元バーコード１４、１５の読取処理は、図７に示した処理と同様である。ただし、この場合、証明情報４６は、必ずしも２次元バーコード１４に出力する必要はなく、署名情報５６に含まれる必要はない。

【００７２】

バーコードリーダ８２は、金融処理装置８１に署名情報の検証と取引の決済を依頼し、処理結果を受け取って利用者に提示する。金融処理装置８１は、データベース８３に登録された情報を用いて、署名情報の正当性を検証する。署名情報の検証処理は、図８に示した処理と同様である。証明情報４６が含まれていない場合は、その検証は省略される。署名情報の正当性が検証されると、金融処理装

置８１は、その取引に関する決済を行う。これにより、例えば、金融機関に設けられた利用者の口座の金銭情報（残高）が変更される。

【００７３】

この署名システムでは、図２の署名システムと異なり、利用者の本人情報のブラインド情報が、取引相手である金融機関により管理され、利用者識別のために用いられる。したがって、本人情報は、銀行印の代わりに使用されると考えられる。

【００７４】

また、取引の安全性をより高めるために、利用者のパスワードをあらかじめデータベース８３に登録しておくこともできる。この場合、利用者は、取引の際に、２次元バーコード１４、１５を提示するとともに、バーコードリーダ８２またはＡＴＭ等の端末を介して、パスワードを金融処理装置８１に入力する。そして、金融処理装置８１は、データベース８３を参照して、入力されたパスワードを検証する。

【００７５】

さらに、図１１の署名システムによれば、端末１１と金融処理装置８１の間で、直接、情報を送受信することで、ホームバンキング／ファームバンキングを実現することもできる。図１２は、このような取引処理を示している。

【００７６】

まず、利用者が端末１１から金融処理装置８１に取引依頼を送信すると、金融処理装置８１は、本人情報３１を端末１１に要求する。これを受けて、利用者が本人情報３１を入力すると、端末１１は、暗号キー３４を用いて本人情報３１を暗号化し、暗号化本人情報９１を生成して、金融処理装置８１に送信する。

【００７７】

金融処理装置８１は、データベース８３に保存された暗号キー３４を用いて暗号化本人情報９１を復号化し、平文の本人情報９２を得る。さらに、データベース８３に保存されたＭＤ関数３２を本人情報９２に適用してＭＤ９３を生成し、それを暗号キー３４で暗号化してブラインド情報９４を生成する。そして、得られたブラインド情報９４をデータベース８３に保存されたブラインド情報３５と

比較する。

【００７８】

このとき、ブラインド情報９４とブラインド情報３５が一致すれば、依頼された取引に関する決済を行い、取引の結果を端末１１に通知する。また、両者が一致しなければ、その決済を行わずに、取引が中止されたことを端末１１に通知する。したがって、利用者が正しい本人情報３１を入力した場合のみ、決済が行われる。また、本人情報９２、ＭＤ９３、およびブラインド情報９４は、使用後直ちに消去される。

【００７９】

図１１の署名システムでは、図２の署名システムと同様に、必要最小限の情報が平文として登録され、本人情報３１は、他人が認識できないブラインド情報３５の形で登録される。したがって、利用者のプライバシーが保護され、他人による本人情報３１の盗用が防止される。

【００８０】

以上説明した実施形態においては、利用者が記憶している意味のある情報を本人情報として用いているが、実印、銀行印、認印等の印影の画像をスキャナ等で取り込み、その画像データを本人情報として用いてもよい。これにより、従来の印鑑とデジタル処理を組み合わせたハイブリッド署名システムが実現される。

【００８１】

また、本人情報を提示するための媒体としては、２次元バーコード以外にも、１次元バーコード、ＩＣ（integrated circuit）メモリカード等の任意の記録媒体を用いることができる。ＩＣメモリカードを用いた場合は、バーコードリーダの代わりに、メモリカードインタフェースを備えた処理装置が用いられる。

【００８２】

さらに、ブラインド情報や暗号化本人情報の生成に共通キー方式の暗号アルゴリズムを用いる必要はなく、暗号化と復号化に異なる暗号キーを用いるＲＳＡ（Rivest-Shamir-Adleman）等の暗号アルゴリズムを用いてもよい。もちろん、ブラインド情報の生成と暗号化本人情報の生成に、それぞれ異なる暗号アルゴリズムを用いることも可能である。

【００８３】

図２の端末１１、バーコードリーダ１２、証明装置１３、図１１の金融処理装置８１、およびバーコードリーダ８２は、例えば、図１３に示すような情報処理装置（コンピュータ）を用いて構成される。図１３の情報処理装置は、ＣＰＵ（中央処理装置）１０１、メモリ１０２、入力装置１０３、出力装置１０４、外部記憶装置１０５、媒体駆動装置１０６、およびネットワーク接続装置１０７を備え、それらはバス１０８により互いに接続されている。

【００８４】

メモリ１０２は、ＲＯＭ（read only memory）、ＲＡＭ（random access memory）等を含み、処理に用いられるプログラムとデータを格納する。ＣＰＵ１０１は、メモリ１０２を利用してプログラムを実行することにより、上述したような署名システムの各処理を行う。

【００８５】

入力装置１０３は、例えば、キーボード、ポインティングデバイス、タッチパネル等であり、必要な指示や情報の入力に用いられる。出力装置１０４は、例えば、ディスプレイやプリンタ等であり、処理結果や２次元バーコード１４、１５等を出力する。

【００８６】

外部記憶装置１０５は、例えば、磁気ディスク装置、光ディスク装置、光磁気ディスク（magneto-optical disk）装置等である。この外部記憶装置１０５に、上述のプログラムとデータを保存しておき、必要に応じて、それらをメモリ１０２にロードして使用することもできる。また、外部記憶装置１０５は、図２のデータベース１６および図１１のデータベース８３としても用いられる。

【００８７】

媒体駆動装置１０６は、可搬記録媒体１０９を駆動し、その記録内容にアクセスする。可搬記録媒体１０９としては、メモリカード、フロッピーディスク、ＣＤ－ＲＯＭ（compact disk read only memory）、光ディスク、光磁気ディスク等、任意のコンピュータ読み取り可能な記録媒体が用いられる。この可搬記録媒体１０９に上述のプログラムとデータを格納しておき、必要に応じて、それらを

メモリ１０２にロードして使用することもできる。

【００８８】

ネットワーク接続装置１０７は、ＬＡＮ（local area network）等の任意のネットワーク（回線）を介して外部の装置と通信する。これにより、必要に応じて、上述のプログラムとデータを外部の装置から受け取り、それらをメモリ１０２にロードして使用することもできる。

【００８９】

図１４は、図１３の情報処理装置にプログラムとデータを供給することのできるコンピュータ読み取り可能な記録媒体を示している。可搬記録媒体１０９や外部のデータベース１１０に保存されたプログラムとデータは、メモリ１０２にロードされる。そして、ＣＰＵ１０１は、そのデータを用いてそのプログラムを実行し、必要な処理を行う。

【００９０】

【発明の効果】

本発明によれば、２次元バーコード等のデジタルデータを用いて、簡単かつ安全に、利用者の識別情報を受領者に提示することができる。また、この識別情報は媒体に保存して管理する必要がなく、使用する度に利用者が入力するため、他人による不正使用を防止することができる。したがって、自筆署名や印鑑を用いる場合より高い安全性が得られる。

【図面の簡単な説明】

【図１】

本発明の署名システムの原理図である。

【図２】

第１の署名システムの構成図である。

【図３】

バーコードリーダの構成図である。

【図４】

登録処理を示す図（その１）である。

【図５】

登録処理を示す図（その２）である。

【図６】

証明書発行処理を示す図である。

【図７】

第１の読取処理を示す図である。

【図８】

検証処理を示す図である。

【図９】

第２の読取処理を示す図である。

【図１０】

署名情報を示す図である。

【図１１】

第２の署名システムの構成図である。

【図１２】

取引処理を示す図である。

【図１３】

情報処理装置の構成図である。

【図１４】

記録媒体を示す図である。

【符号の説明】

１　入力手段

２　出力手段

３　読取手段

４　生成手段

１１　端末

１２、８２　バーコードリーダ

１３　証明装置

１４、１５　２次元バーコード

１６、８３、１１０　データベース

２１　読取装置

２２　通信装置

２３　制御装置

２４　記憶装置

２５　表示装置

２６　タイマ

２７　乱数発生器

３１、３８、４２、５７、９２　本人情報

３２　メッセージダイジェスト関数

３３、３９、４３、５４、５８、６２、７４、７５、７６、９３　メッセージダイジェスト

３４　暗号キー

３５、４０、４４、５５、５９、６０、６３、７７、７８、７９、９４　ブラインド情報

３６　本人証明書

３７、４１、５１、９１　暗号化本人情報

４５、６１　付加情報

４６　証明情報

５２、７１　署名プログラム

５３、７３　使用情報

５６、８０　署名情報

７２　テスト情報

８１　金融処理装置

１０１　ＣＰＵ

１０２　メモリ

１０３　入力装置

１０４　出力装置

１０５　外部記憶装置

１０６　媒体駆動装置

１０７　ネットワーク接続装置

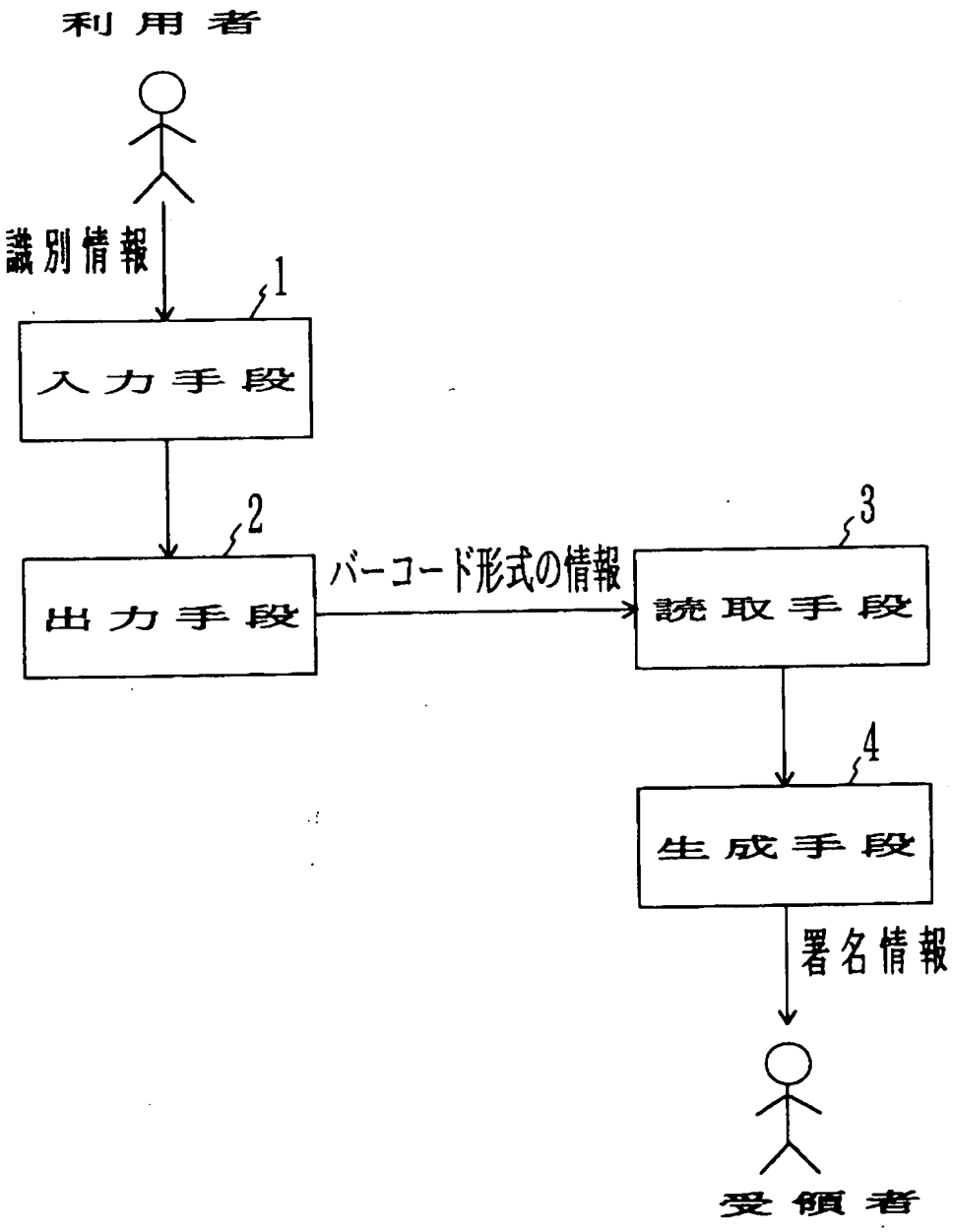
１０８　バス

１０９　可搬記録媒体

【書類名】　　図面

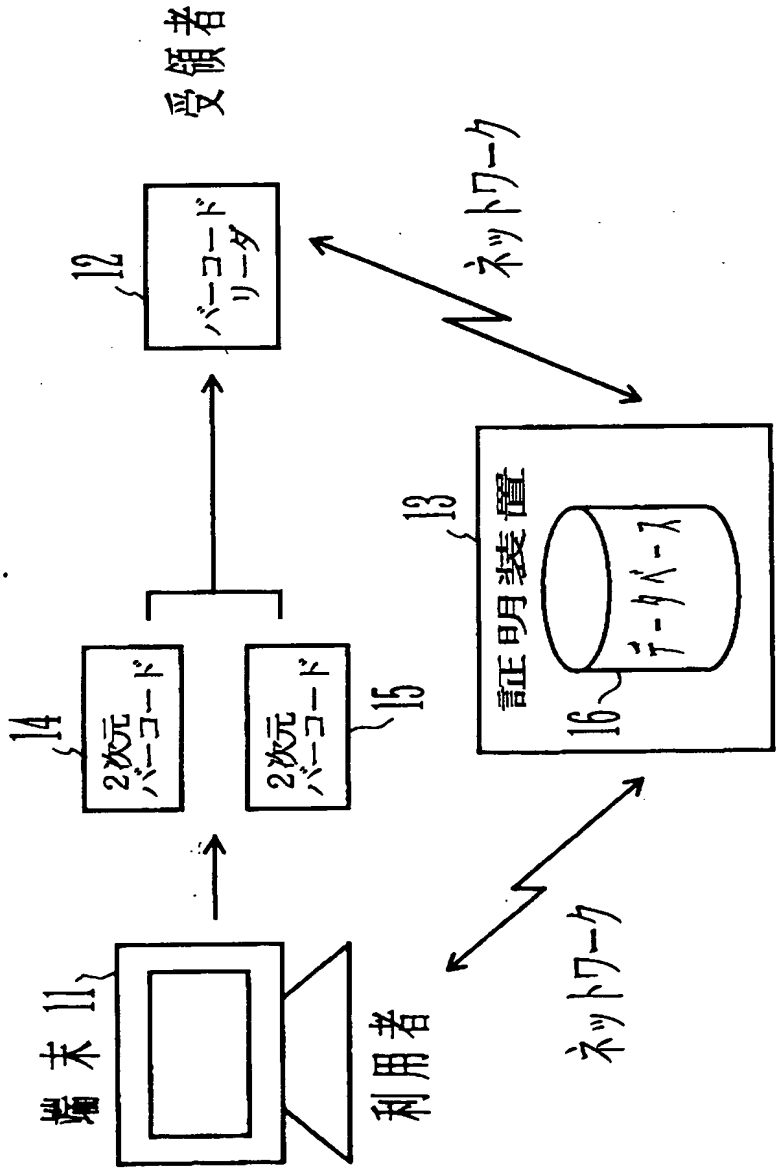
【図１】

本　発　明　の　原　理　図



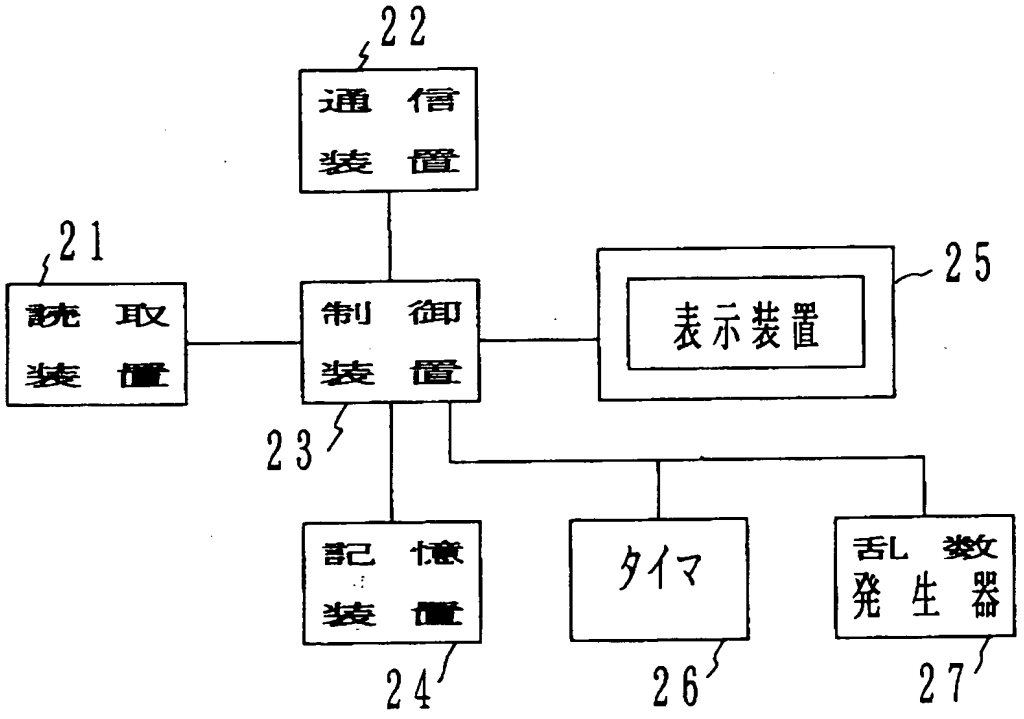
【図２】

第１の署名システムの構成図



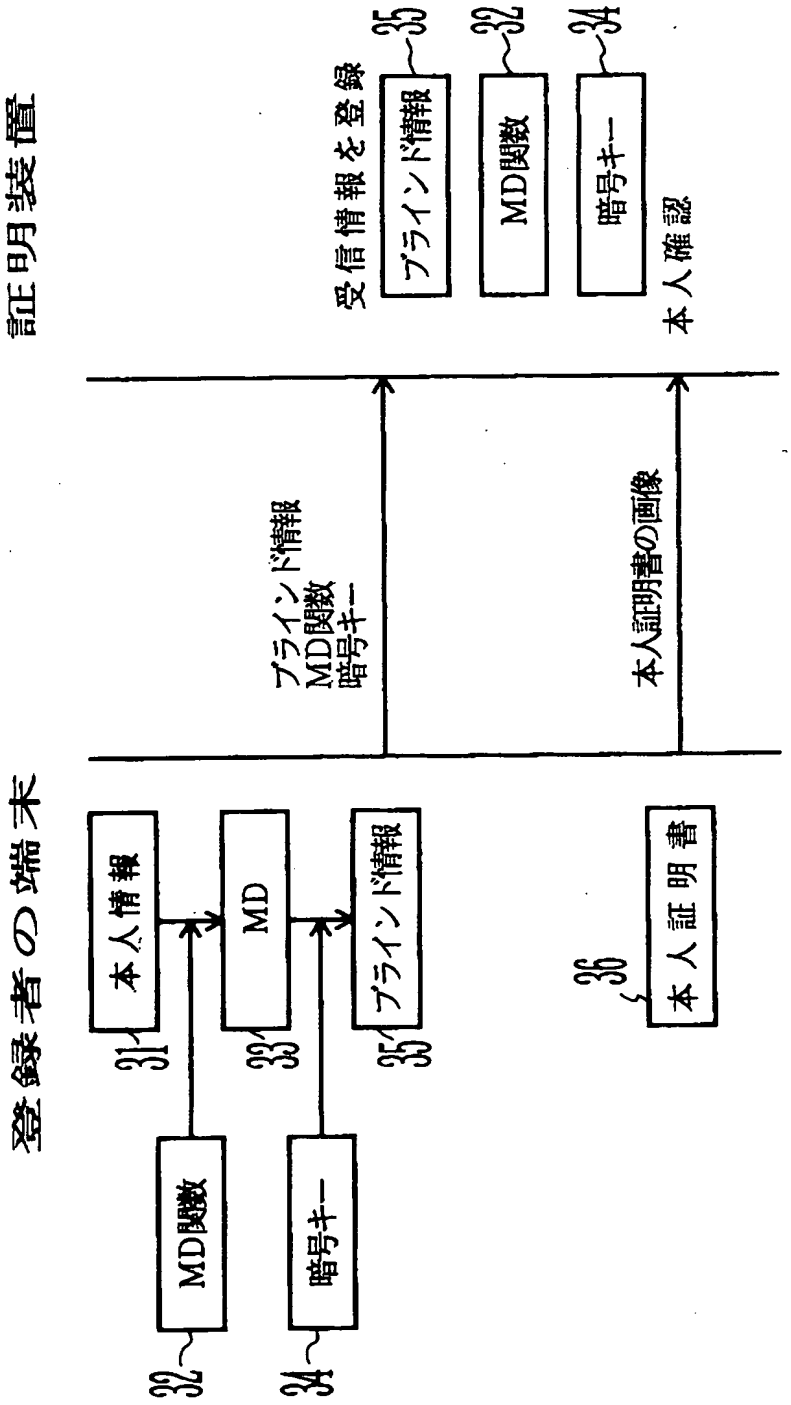
【図３】

バーコードリーダの構成図



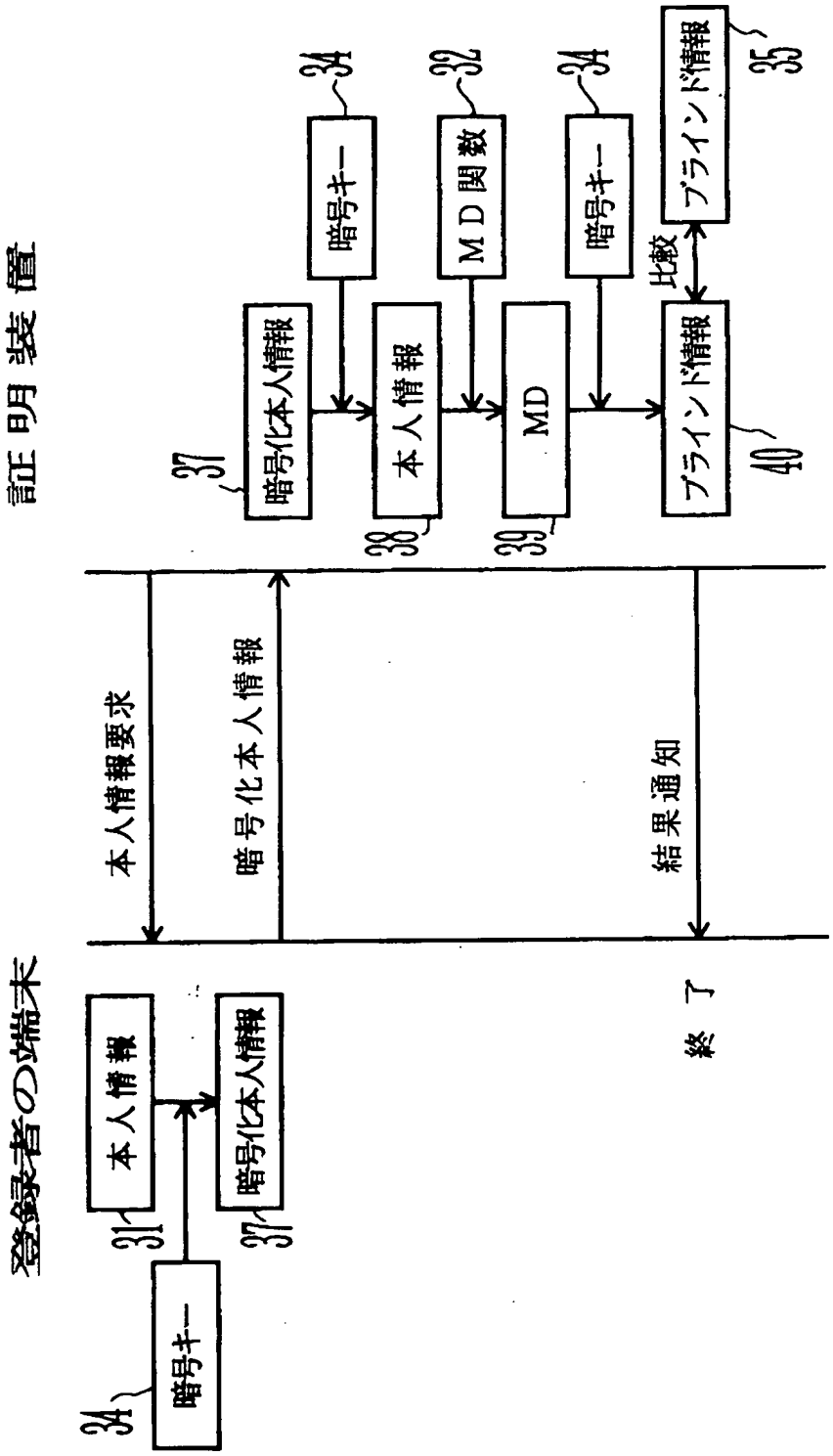
【図４】

登録処理を示す図（その１）



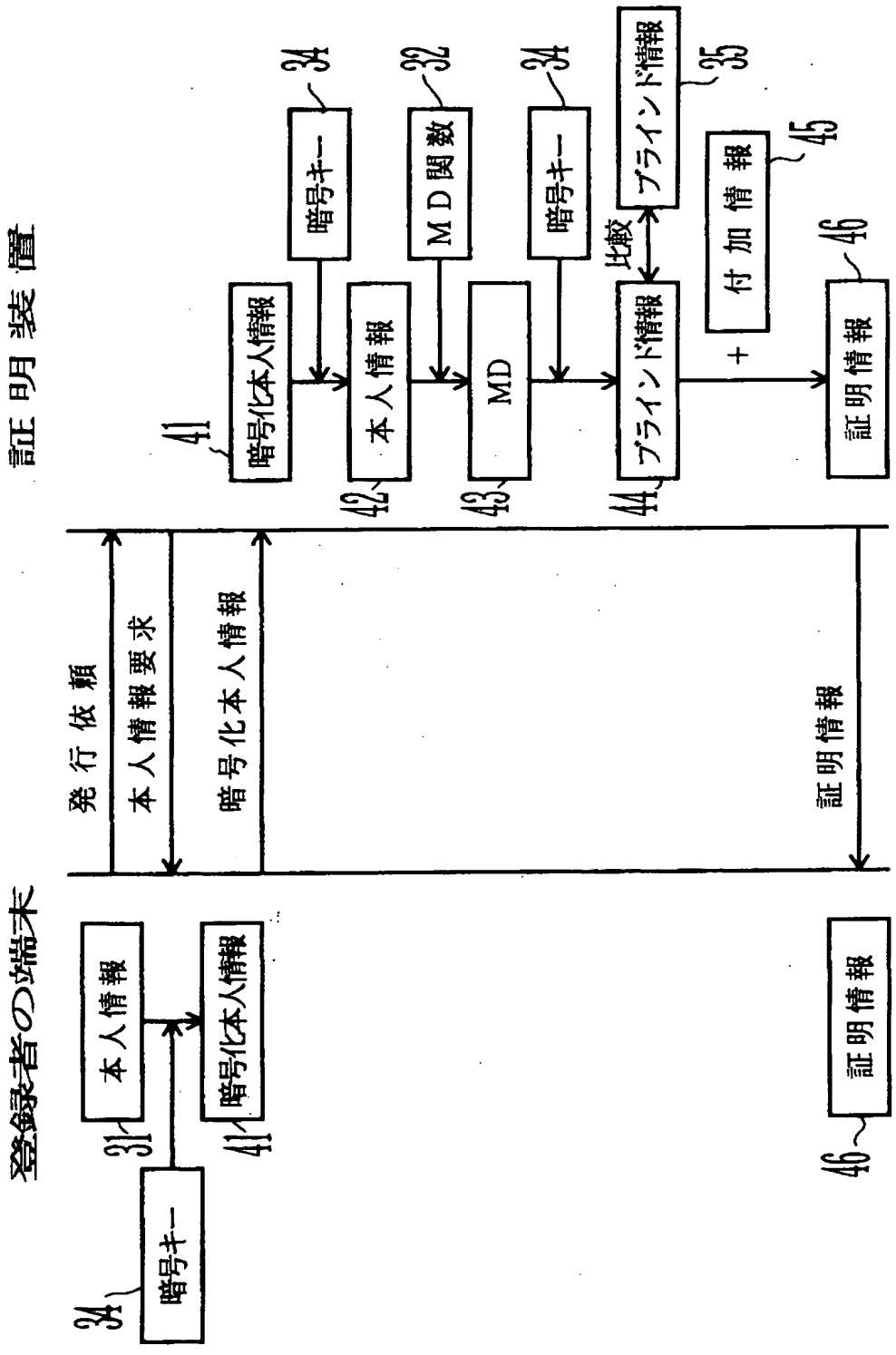
【図５】

登録処理を示す図（その2）



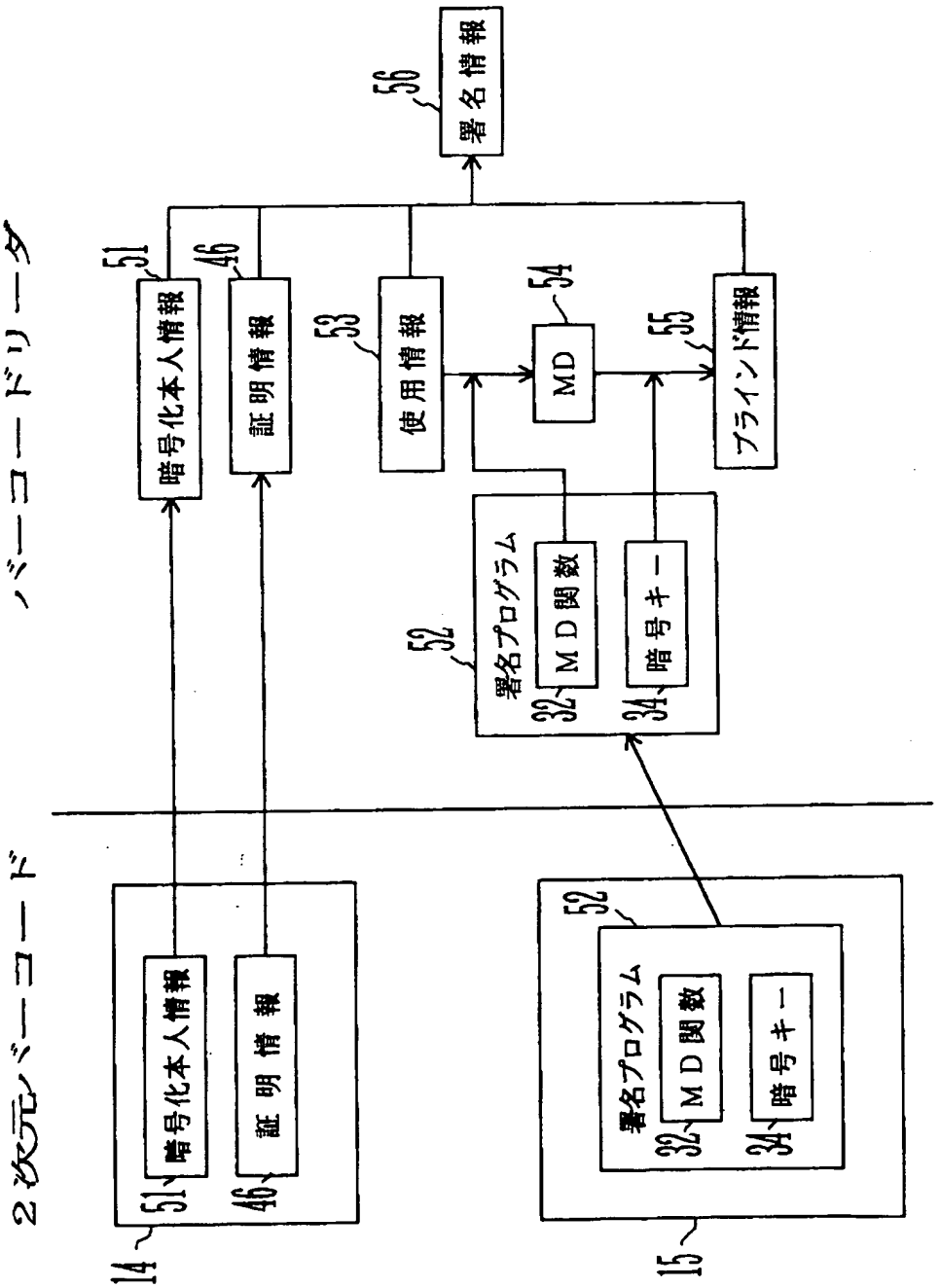
【図６】

証明書発行処理を示す図



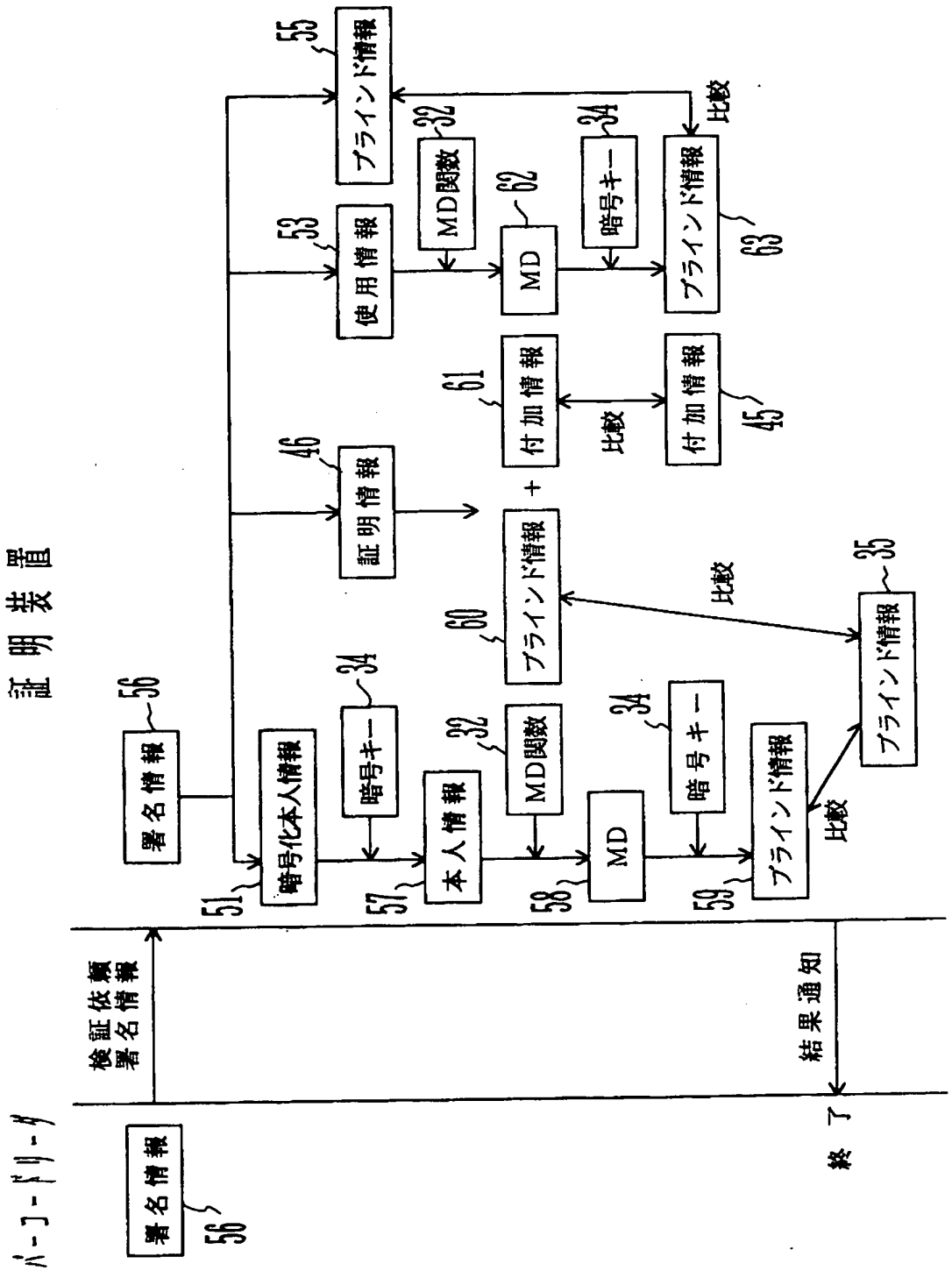
【図７】

第1の読取処理を示す図



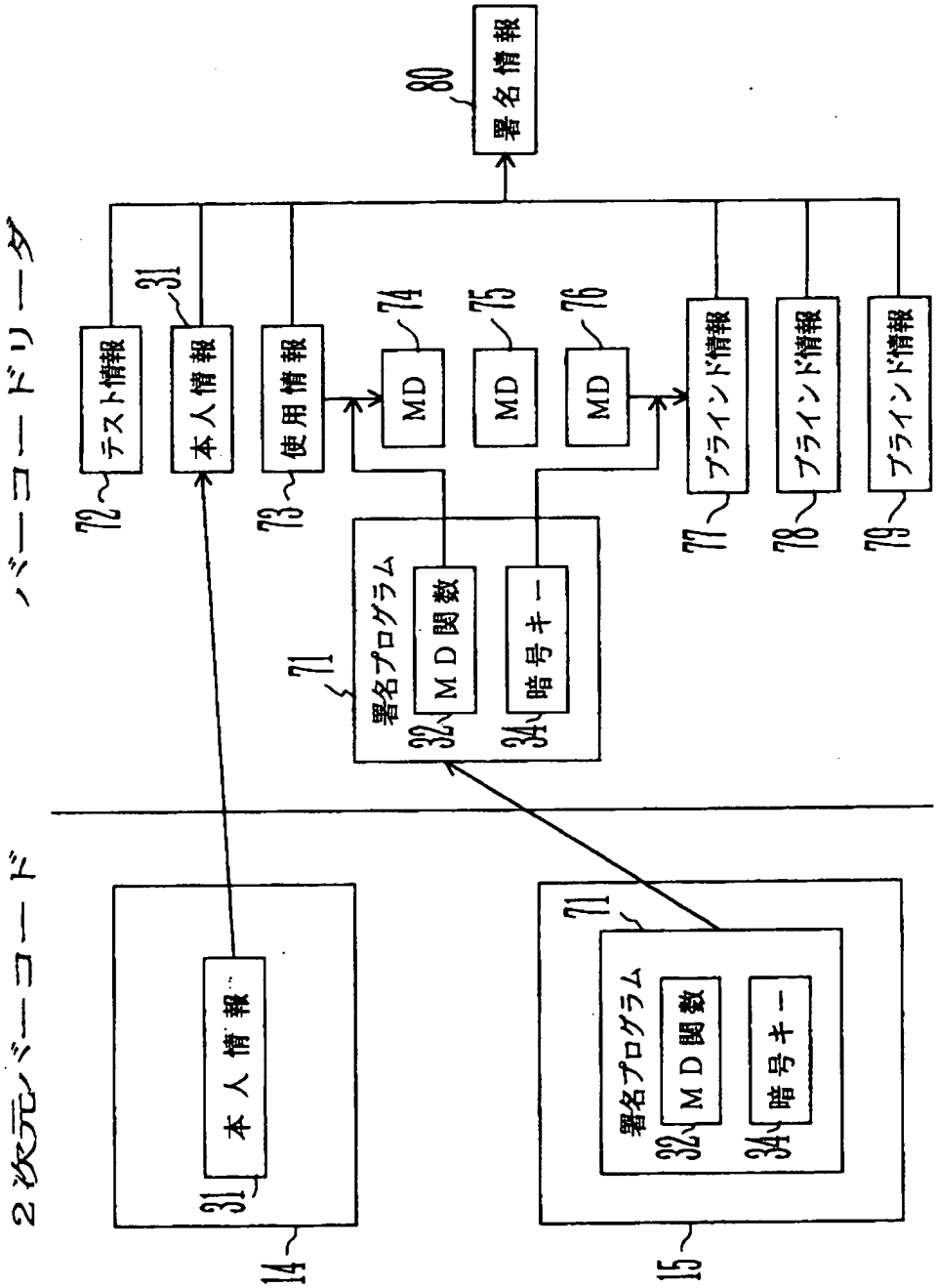
【図８】

検証処理を示す図


証明装置
パーコードリーダ
署名情報
56
検証依頼
署名情報
署名情報
56
暗号化本人情報
51
暗号キー
34
署名情報
56
本人情報
57
MD関数
32
MD
58
暗号キー
34
ブラインド情報
59
ブラインド情報
55
使用情報
53
MD関数
32
MD
62
暗号キー
34
ブラインド情報
63
比較
証明情報
46
付加情報
61
比較
付加情報
45
+
ブラインド情報
60
比較
ブラインド情報
35
比較
結果通知
終了

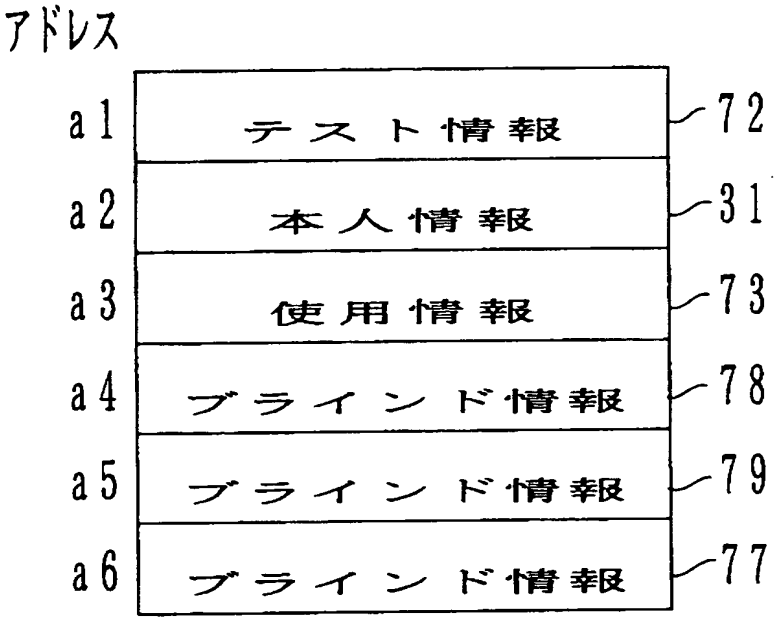
【図９】

第２の読取処理を示す図



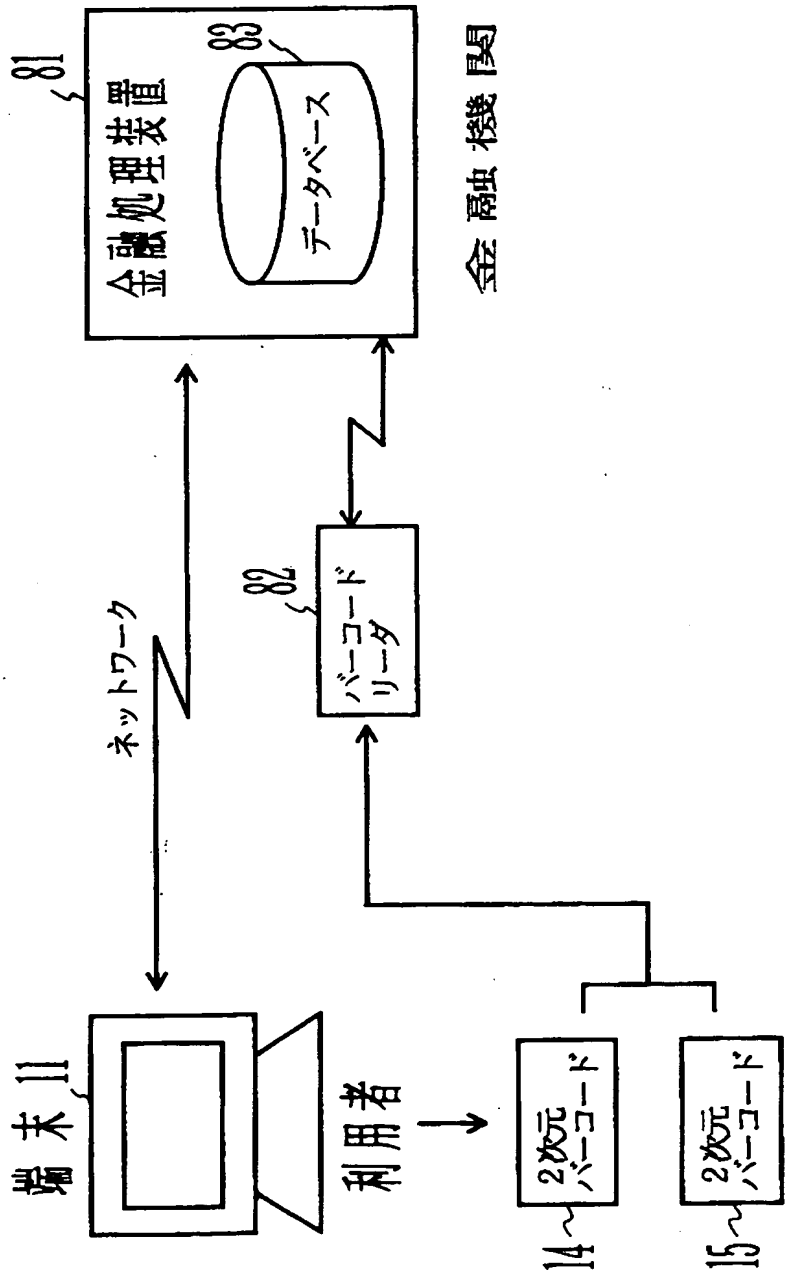
【図１０】

署名情報を示す図



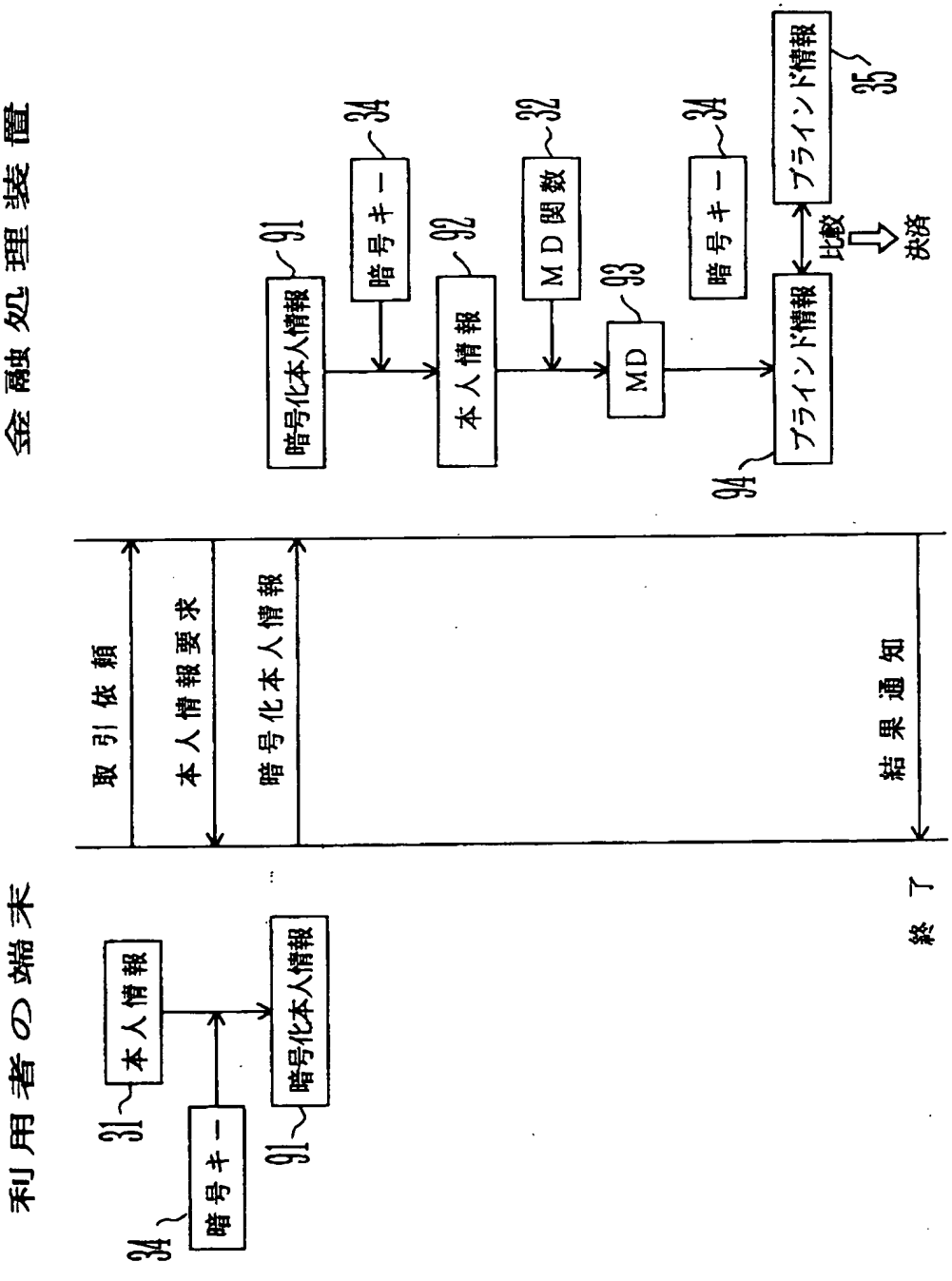
【図１１】

第2の署名システムの構成図



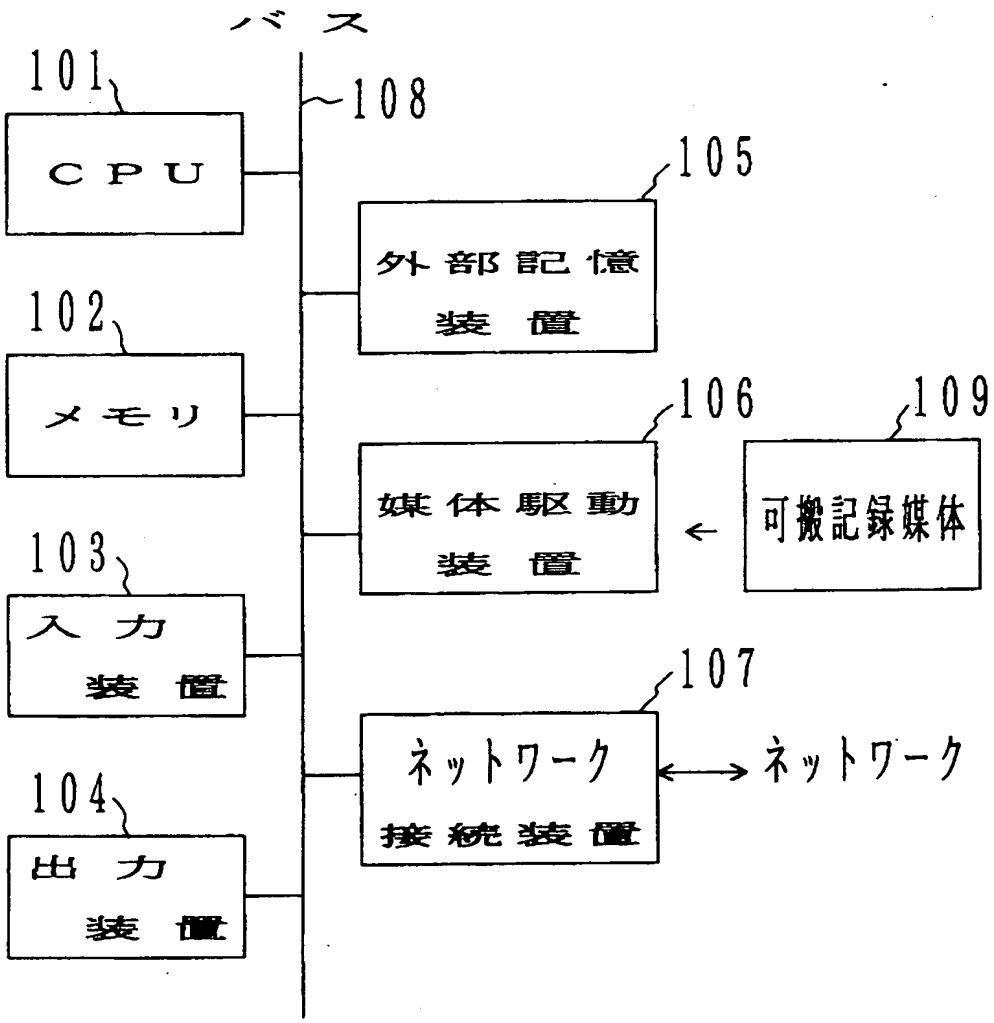
【図１２】

取引処理を示す図


利用者の端末
金融処理装置
本人情報
暗号キー
暗号化本人情報
31
34
91
取引依頼
本人情報要求
暗号化本人情報
結果通知
終了
暗号化本人情報
暗号キー
本人情報
MD関数
MD
暗号キー
ブラインド情報
ブラインド情報
比較
決済
91
34
92
32
93
34
94
35

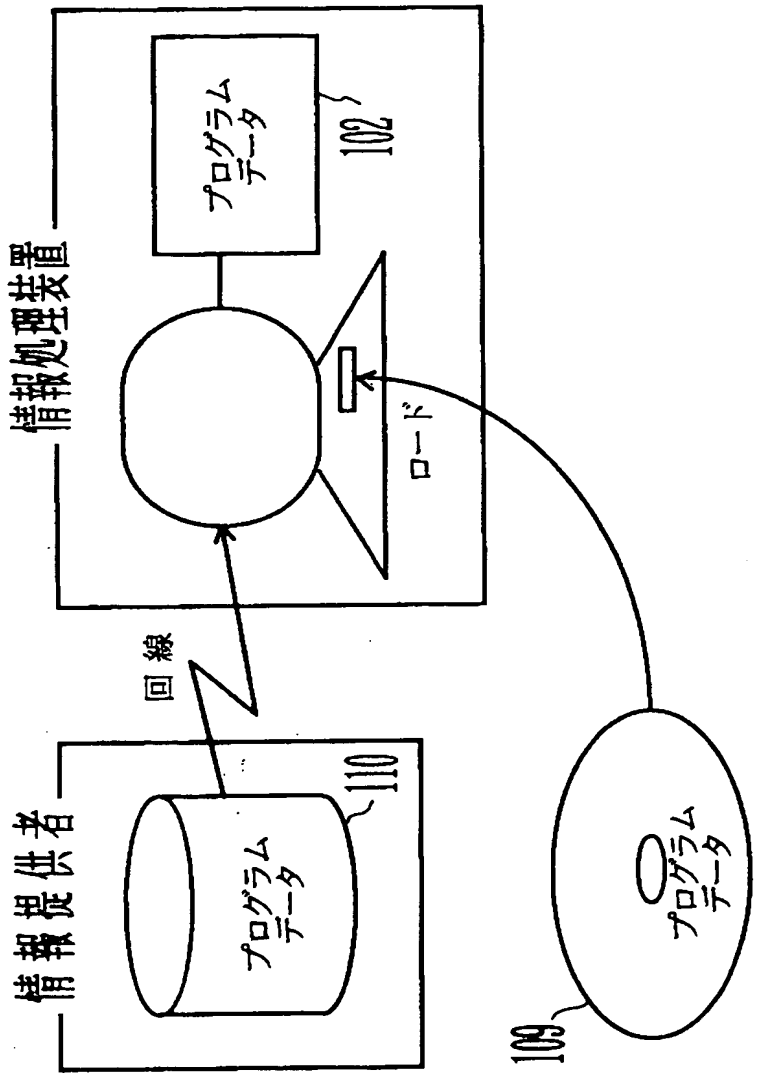
【図１３】

情報処理装置の構成図



【図１４】

記録媒体を示す図



【書類名】　要約書

【要約】

【課題】　情報処理装置を用いて利用者の識別情報を受領者に提示し、それを安全に管理することが課題である。

【解決手段】　利用者は、端末１１に識別情報を入力して、識別情報の２次元バーコード１４と署名プログラムの２次元バーコード１５を生成する。受領者は、バーコードリーダ１２を用いて２次元バーコード１４、１５を読み取り、バーコードリーダ１２は、署名プログラムを実行して、識別情報を含む署名情報を生成する。証明装置１３は、バーコードリーダ１２からの依頼を受けて、署名情報を検証し、結果をバーコードリーダ１２に通知する。

【選択図】　図２

【書類名】　職権訂正データ
【訂正書類】　特許願

＜認定情報・付加情報＞
【特許出願人】
【識別番号】　000005223
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号
【氏名又は名称】　富士通株式会社
【特許出願人】
【識別番号】　596089344
【住所又は居所】　東京都千代田区九段南１丁目３番１号
【氏名又は名称】　株式会社さくら銀行
【代理人】　申請人
【識別番号】　100074099
【住所又は居所】　東京都千代田区二番町８番地２０　二番町ビル３Ｆ　大菅内外国特許事務所
【氏名又は名称】　大菅　義之
【選任した代理人】
【識別番号】　100067987
【住所又は居所】　神奈川県横浜市港北区太尾町１４１８－３０５　（大倉山二番館）　久木元特許事務所
【氏名又は名称】　久木元　彰

出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　　富士通株式会社

出　願　人　履　歴　情　報

識別番号　　〔５９６０８９３４４〕

１．変更年月日　　１９９６年　６月２０日
［変更理由］　新規登録
住　所　東京都千代田区九段南１丁目３番１号
氏　名　株式会社さくら銀行